ワイヤレスLANコントローラ(WLC)でのWeb認証について

内容

概要

このドキュメントでは、ワイヤレスLANコントローラ(WLC)でのWeb認証のプロセスについて説明します。

前提条件

要件

WLC 設定に関する基本的な知識があることをお勧めします。

使用するコンポーネント

このドキュメントの情報は、すべての WLC ハードウェア モデルに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Web 認証の内部プロセス

Web 認証のセキュリティ機能としての位置付け

Web 認証（WebAuth）はレイヤ 3 セキュリティです。これは、ブラウザを実行する任意のステーションで機能する使いやすいセキュリティを提供します。

任意の事前共有キー(PSK)セキュリティ（レイヤ2セキュリティポリシー）と組み合わせることができます。

WebAuthとPSKの組み合わせによってユーザフレンドリな部分が減少しますが、クライアントトラフィックを暗号化する利点があります。

WebAuth は、暗号化のない認証方法です。

WLCソフトウェアリリース7.4をインストールして同時に設定するまでは、WebAuthを802.1x/RADIUS(Remote Authentication Dial-In User Service)で設定することはできません。

クライアントは、dot1x認証とWeb認証の両方を通過する必要があります。これは、ゲストではなく、従業員用のWebポータル（802.1xを使用）の追加を目的としています。

従業員またはゲストの Web ポータルの dot1x に対するオールインワンの Service Set Identifier（SSID）はありません。

WebAuth の動作の仕組み

802.11 認証プロセスはオープンであるため、認証および関連付けを問題なく行うことができます。その後、関連付けられますが、WLCでは関連付けられません **RUN** 変わります。

Web認証が有効な場合は、 **WEBAUTH_REQD** ネットワークリソースにアクセスできない。

オプションにDNSサーバのアドレスを含むDHCP IPアドレスを受信する必要があります。

ブラウザで有効なURLを入力してください。クライアントは、DNS プロトコルを介して URL の名前解決を行います。次に、クライアントは、その HTTP 要求を Web サイトの IP アドレスに送信します。

WLCはその要求を代行受信し、 **webauth** WebサイトのIPアドレスを模倣するログインページ。外部WebAuthでは、WLCはWebサイトのIPアドレスを含むHTTP応答で応答し、ページが移動したことを示します。

ページは、WLC により使用される外部 Web サーバに移動されます。認証されると、すべてのネットワークリソースにアクセスできるようになり、デフォルトでは最初に要求されたURLにリダイレクトされます（WLCで強制リダイレクトが設定されていない場合）。

要約すると、WLCではクライアントがDNSを解決し、IPアドレスを自動的に **WEBAUTH_REQD** 変わります。

ポート80ではなく別のポートを監視するには、 **config network web-auth-port** このポートにもリダイレクトを作成します。

たとえば、ポート 2002 を使用する Access Control Server（ACS）Web インターフェイスやその他の同様のアプリケーションです。

> **HTTPSリダイレクションに関する注意**：デフォルトでは、WLCはHTTPSトラフィックをリダイレクトしませんでした。つまり、ブラウザにHTTPSアドレスを入力しても何も起こりません。HTTPSで提供されたログインページにリダイレクトするには、HTTPアドレスを入力する必要があります。
>
> バージョン8.0以降では、CLIコマンドを使用してHTTPSトラフィックのリダイレクトを有効にできます **config network web-auth https-redirect enable.**
>
> これにより、多数のHTTPS要求が送信される場合に、WLCで多くのリソースが使用されます。この機能のスケーラビリティが強化されたWLCバージョン8.7より前にこの機能を使用することは推奨されません。また、この場合は証明書の警告が避けられないことに注意してください。クライアントがURL(https://www.cisco.comなど)を要求した場合でも、WLCは仮想インターフェイスのIPアドレスに対して発行された独自の証明書を提示します。これは、クライアントが要求したURL/IPアドレスと一致せず、クライアントがブラウザで例外を強制しない限り、証明書は信頼されません。

8.7より前のWLCソフトウェアリリースの指標となるパフォーマンス低下を測定しました。

WebAuth	達成率
3つのURL:HTTP	140/秒
最初のURL:HTTP 第2および第3のURL:HTTPS	20/秒
3つのURL:HTTPS（大規模導入）	<1/秒
3つのURL:HTTPS（最大100クライアント）	10/秒

このパフォーマンス表では、3つのURLを次のように示します。

- エンドユーザが入力した元のURL
- WLCがブラウザをリダイレクトするURL
- 最終的な資格情報の送信

パフォーマンステーブルは、3つのURLがすべてHTTPの場合、3つのURLがすべてHTTPSの場合、またはクライアントがHTTPからHTTPSに移動した場合（通常）にWLCのパフォーマンスを示します。

内部ページで内部（ローカル）WebAuth を動作させる方法

WLANに動作可能なダイナミックインターフェイスを設定するために、クライアントはDHCPを通じてDNSサーバのIPアドレスも受け取ります。

先に **webauth** が設定されている場合は、WLANが正しく動作していることを確認します。DNS要求を解決できます(**nslookup**)を参照し、Webページを参照できます。

Web認証をレイヤ3セキュリティ機能として設定します。ローカルデータベースまたは外部RADIUSサーバにユーザを作成します。

詳細については、「ワイヤレス LAN コントローラ（WLC）上の Web 認証の設定例」を参照してください。

カスタム ページでカスタムのローカル WebAuth を設定する方法

Custom **webauth** 次のように設定できます。 **redirectUrl Security** tab.これにより、入力した特定のWebページに強制的にリダイレクトされます。

ユーザが認証されると、クライアントが要求した元のURLが上書きされ、リダイレクトが割り当てられたページが表示されます。

カスタム機能を使用すると、デフォルトのログイン ページではなく、カスタム HTML ページを使用できます。HTML およびイメージ ファイル バンドルがコントローラにアップロードされます。

アップロードページで、 **webauth bundle** tar形式で保存します。PicoZipは、WLCと互換性のあるtarを作成します。

WebAuth バンドルの例については、「ワイヤレス コントローラ WebAuth バンドルのソフトウェアのダウンロード」ページを参照してください。WLCに適したリリースを選択します。

既存のバンドルをカスタマイズすることをお勧めします。新しいバンドルを作成しないでください。

～にはいくつかの制限がある。 **custom webauth** これはバージョンやバグによって異なります。

- .tarファイルのサイズ（5MB以下）
- .tar のファイル数
- ファイルのファイル名の長さ（30文字以内）

パッケージが動作しない場合は、単純なカスタムパッケージを試してみてください。ユーザが使用しようとしたパッケージに到達するために、ファイルと複雑さを個別に追加します。これは問題を特定するのに役立ちます。

カスタムページを設定するには、『CiscoワイヤレスLANコントローラコンフィギュレーションガイド、リリース7.6』の「カスタマイズされたWeb認証ログインページの作成」を参照してください。

グローバル設定をオーバーライドする手法

override global configコマンドを使用して設定し、各WLANのWebAuthタイプを設定します。これにより、別のWLANに対して、内部/デフォルトWebAuthとカスタム内部/デフォルトWebAuthが許可されます。

これにより、WLANごとに異なるカスタムページを設定できます。

すべてのページを同じバンドルにまとめて、WLCにアップロードします。

各WLANで**override global config**コマンドを使用してカスタムページを設定し、バンドル内のすべてのファイルからログインページにするファイルを選択します。

各WLANのバンドル内で異なるログインページを選択します。

リダイレクションの問題

HTML バンドルには、リダイレクションを可能にする変数があります。ここに強制リダイレクション URL を含めないでください。

カスタムWebAuthでのリダイレクションの問題については、バンドルを確認することをお勧めします。

WLC GUI に **+=** を使用するリダイレクト URL を入力すると、バンドル内で定義されている URL でオーバーライドされるか、これに追加されます。

たとえば、WLC GUIでは、 **redirectURL** フィールドはwww.cisco.comに設定されます。バンドルでは、次のように表示されます。 **redirectURL+=**「(webサイトのURL)」。 **+=**を指定すると、ユーザは無効なURLにリダイレクトされます。

外部ページで外部（ローカル）Web 認証を動作させる方法

外部WebAuthサーバの利用は、ログインページの外部リポジトリにすぎません。ユーザ クレデンシャルは、WLC により認証されます。外部Webサーバでは、特別なログインページまたは別のログインページだけが許可されます。

外部WebAuthに対して実行される手順：

1. クライアント（エンド ユーザ）が Web ブラウザを開き、URL を入力します。

2. このクライアントが認証されず、外部 Web 認証が使用される場合、WLC は、このユーザを外部 Web サーバ URL にリダイレクトします。WLCは、模倣されたIPアドレスを使用してHTTPリダイレクトをクライアントに送信し、外部サーバのIPアドレスをポイントします。外部Web認証のログインURLには、次のようなパラメータが追加されます。**AP_Mac_Address**,ページ **client_url** (**クライアントURLアドレス**)、 **action_URL** スイッチのWebサーバに接続するために必要です。

3. 外部 Web サーバ URL は、ユーザをログイン ページに送信します。ユーザは、事前認証アクセスコントロールリスト(ACL)を使用してサーバにアクセスできます。

4. ログインページは、ユーザクレデンシャル要求を **action_URL**たとえば、WLC Webサーバのhttp://192.0.2.1/login.htmlなどです。これはリダイレクトURLへの入力パラメータとして提供

されます。ここで、192.0.2.1はスイッチの仮想インターフェイスアドレスです。

5. WLC Web サーバは、認証のためにユーザ名とパスワードを送信します。

6. WLC は RADIUS サーバ要求を開始するか、WLC 上のローカル データベースを使用してユーザを認証します。

7. 認証が成功した場合、WLC Web サーバは、設定されたリダイレクト URL またはクライアントが入力した URL にユーザを転送します。

8. 認証が失敗すると、WLC Webサーバはユーザをユーザログインurlにリダイレクトして戻します。

   注：このドキュメントでは、仮想IPの例として192.0.2.1を使用します。192.0.2.xの範囲はルーティング不可能であるため、仮想ipに使用することを推奨します。古いドキュメントでは、おそらく「1.1.1.x」を参照するか、これがデフォルト設定として使用されたWLCで設定されたままの状態になっています。ただし、このipは有効なルーティング可能ipアドレスになったため、代わりに192.0.2.xサブネットが推奨されることに注意してください。

アクセスポイント(AP)がFlexConnectモードの場合、 **preauth** ACLは無関係です。認証されないクライアントに Web サーバへのアクセスを許可するには、Flex ACL を使用できます。

「ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例」を参照してください。

Web パススルー

Webパススルーは、内部Web認証の一種です。Web パススルーでは、警告またはアラート ステートメントを示すページが表示され、クレデンシャル プロンプトは表示されません。

次に、ユーザが[ok] をクリックします。電子メール入力を有効にすると、ユーザはユーザ名となる電子メールアドレスを入力できます。

ユーザが接続したら、アクティブクライアントリストを確認し、ユーザがユーザ名として入力した電子メールアドレスでリストされていることを確認します。

詳細は、『ワイヤレスLANコントローラ5760/3850 Webパススルーの設定例』を参照してください。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。

リダイレクト ページ、および、RADIUS サーバでリダイレクトを実行する条件を指定できます。

パスワードが有効期限に達した場合、またはユーザが引き続き使用またはアクセスするために料金を支払う必要がある場合は、条件にパスワードを含めることができます。

RADIUSサーバがCisco AVペアを返す場合、 **url-redirect**ユーザがブラウザを開くと、指定した

URLにリダイレクトされます。

サーバがCisco AVペアも返す場合、 **url-redirect-acl**次に、指定したACLがこのクライアントの事前認証ACLとしてインストールされます。

クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。指定されている URL でクライアントが特定の操作 (パスワードの変更や料金の支払いなど) を完了した後で、クライアントは再度認証を行う必要があります。

RADIUSサーバがRADIUSサーバから **url-redirect**クライアントは完全に認証され、トラフィックの通過が許可されていると見なされます。

> **注**：条件付き Web リダイレクト機能は、802.1x または WPA+WPA2 レイヤ 2 セキュリティ用に設定されている WLAN でのみ使用できます。

RADIUSサーバの設定後、コントローラのGUIまたはCLIを使用して、条件付きWebリダイレクトをコントローラに設定します。次の詳細手順を示したガイドを参照してください。Webリダイレクトの設定(GUI)およびWebリダイレクトの設定(CLI)。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークにフル アクセスできます。

RADIUS サーバでリダイレクト ページを指定できます。RADIUSサーバがCisco AVペアを返す場合、 **url-redirect**ユーザがブラウザを開くと、指定したURLにリダイレクトされます。

この時点でクライアントは完全に認証されていると見なされ、RADIUSサーバがRADIUSサーバからのIPアドレスを返さなくても、 **url-redirect.**

> **注**：スプラッシュページリダイレクト機能は、802.1xまたはWPA+WPA2レイヤ2セキュリティが設定されたWLANでのみ使用できます。

RADIUSサーバの設定後、コントローラのGUIまたはCLIを使用して、コントローラ上でスプラッシュページWebリダイレクトを設定します。

MAC フィルタ失敗時の WebAuth

MACフィルタFaFailureのWebAuthでは、レイヤ2セキュリティメニューでMACフィルタを設定できます。

ユーザがMACアドレスを使用して正常に検証された場合、ユーザは **run** 変わります。

そうでない場合は、 **WEBAUTH_REQD** 通常のWeb認証が行われます。

> **注**：これはWebパススルーではサポートされていません。詳細については、拡張要求Cisco Bug ID CSCtw73512のアクティビティを参照してください。

中央 Web 認証

中央 Web 認証は、WLC がサービスをホストしない状況で使用されます。クライアントはISE Webポータルに直接送信され、WLC上の192.0.2.1を通過しません。ログイン ページおよびポータル全体は外部に配置されます。

中央 Web 認証は、RADIUS ネットワーク アドミッション コントロール（NAC）を WLAN の詳細設定で有効にし、MAC フィルタを有効にしている場合に発生します。

WLCはRADIUS認証（通常はMACフィルタ用）をISEに送信し、ISEはRADIUS認証に応答して **redirect-url** 属性値(AV)ペア。

その後、ユーザを入力します **POSTURE_REQD** iseが認可変更(CoA)要求による認可を与えるまで状態を続けます。同様のことは、Posture または Central WebAuth でも発生します。

中央 WebAuth は、WPA-Enterprise/802.1x には対応しません。これは、拡張認証プロトコル（EAP）の場合のようにゲスト ポータルが暗号化キーのセッションキーを返すことができないためです。

外部ユーザ認証（RADIUS）

外部ユーザ認証(RADIUS)は、WLCがクレデンシャルを処理する場合、またはレイヤ3 Webポリシーが有効になっている場合にのみ、ローカルWeb認証に対して有効です。ローカルまたはWLC上で、あるいはRADIUS経由で外部からユーザを認証します。

WLC は次の順にユーザのクレデンシャルをチェックします。

1. いずれの場合でも、独自のデータベースが参照されます。
2. そこでユーザが見つからない場合、ゲスト WLAN で設定されている RADIUS サーバがチェックされます。
3. 次に、グローバルRADIUSサーバリストをRADIUSサーバと照合してチェックします。ここで、 **network user** チェックが入っていることを確認します。

この3番目のポイントは、そのWLANに対してRADIUSを設定しないユーザの質問に対する回答ですが、コントローラ上でユーザが見つからない場合でもRADIUSに対してチェックされることに注意してください。

これは、 **network user** は、グローバルリストのRADIUSサーバに対してチェックされます。

WLC は、パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）または EAP-MD5（メッセージ ダイジェスト 5）でユーザを RADIUS サーバに認証できます。

これは、グローバル パラメータで、GUI または CLI から設定できます。

GUI から：移動 **Controller > Web RADIUS Authentication**

CLI から：enter **config custom-web RADIUSauth**

注:NACゲストサーバはPAPのみを使用します。

有線ゲスト WLAN の設定方法

有線ゲストWLANの設定は、ワイヤレスゲストの設定に似ています。1つまたは2つのコントローラで設定できます（1つが自動アンカーの場合のみ）。

有線ゲストユーザのVLANとして、VLAN 50などのVLANを選択します。有線ゲストがインターネットにアクセスする場合は、VLAN 50に設定されたスイッチ上のポートにラップトップを接続します。

この VLAN 50 は、WLC トランク ポートを介したパスで許可し、そこに存在する必要があります。

2 つの WLC（アンカーと外部）を使用する場合、この有線ゲスト VLAN は、アンカーではなく、外部 WLC（WLC1）に接続する必要があります。

次に、WLC1はDMZ WLC（WLC2という名前のアンカー）へのトラフィックトンネルを処理します。DMZ WLCはルーテッドネットワークでトラフィックを解放します。

次に、有線ゲスト ユーザ アクセスを設定する 5 つのステップを示します。

1. **有線ゲスト ユーザ アクセス用の動的インターフェイス（VLAN）を設定します。**

   WLC1で、ダイナミックインターフェイスVLAN50を作成します。 **interface configuration** ページで、 **Guest LAN** ボックス次に、次のようなフィールドが表示されます **IP address** と **gateway** 消えろ。WLCは、トラフィックがVLAN 50からルーティングされることを認識する必要があります。これらのクライアントは有線ゲストです。

2. **ゲスト ユーザ アクセス用の有線 LAN を作成します。**

   コントローラで、インターフェイスは、WLAN に関連付けられる場合に使用されます。次に、本社のコントローラでWLANを作成します。移動先 **WLANs** をクリックし、 **New.**イン **WLAN Type**,選択 **Guest LAN.**

   [Profile Name] および [WLAN SSID] で、この WLAN を識別する名前を入力します。これらの名前を変更できますが、スペースを含めることはできません。WLAN という名前が使用されますが、このネットワーク プロファイルはワイヤレス ネットワーク プロファイルには関連しません。

   「 **General** タブには、次の2つのドロップダウンリストがあります。 **Ingress** と **Egress.**[Ingress] は、ユーザが送信される VLAN です（VLAN 50）。Egressは送信先のVLANです。

   を参照 **Ingress**,選択 **VLAN50.**

   を参照 **Egress**異なります。コントローラが1つだけの場合は、別のダイナミックインターフェイスである **standard** （ゲストLANではなく）一度だけ接続し、有線ユーザをこのインターフェイスに送信します。この場合、DMZ コントローラに送信します。したがって、 **Egress** インターフェイスを選択し、 **Management Interface.**

「 **Security** このゲストLAN「WLAN」のモードはWebAuthであり、これは許容されます。クリック **Ok** 検証します。

3. **外部コントローラ（本社）を設定します。**

WLAN listをクリックし、 **Mobility Anchor** 最後に **Guest LAN** DMZコントローラを選択します。ここでは、両方のコントローラが互いを認識することを前提としています。そうでない場合は、 **Controller** > **Mobility Management** > **Mobility group**WLC1に**DMZWLC**を追加し、DMZに**WLC1**を追加します。両方のコントローラが同じモビリティグループに属していないこと。同じ場合、基本セキュリティ規則に違反します。

4. **アンカー コントローラ（DMZ コントローラ）を設定します。**

本社のコントローラの準備ができました。DMZコントローラを準備します。DMZ コントローラに Web ブラウザ セッションを開き、[WLANs] に移動します。新規 WLAN を作成してください。イン **WLAN Type**,選択 **Guest LAN**.

イン **Profile Name** と **WLAN SSID**、このWLANを識別する名前を入力します。本社コントローラと同じ値を入力します。

「 **Ingress** インターフェイス **None**.トラフィックはEthernet over IP(EoIP)トンネルを介して受信されるため、これは重要ではありません。入力インターフェイスを指定する必要はありません。

「 **Egress** インターフェイスは、クライアントが送信される場所です。たとえば、 **DMZ VLAN** はVLAN 9です。DMZWLC上にVLAN 9の標準ダイナミックインターフェイスを作成し、 **VLAN 9** 出力インターフェイスとして設定します。

モビリティアンカートンネルの終端を設定します。[WLAN] リストから、 **Mobility Anchor for Guest LAN**.トラフィックをローカル コントローラ **DMZWLC** に送信します。これで、両端の準備ができました。

5. **ゲスト LAN を調整します。**

両端の WLAN 設定を調整することもできます。設定は両端で同じである必要があります。たとえば、 **WLAN Advanced** tab, **Allow AAA override** wlc1で、DMZWLCと同じチェックボックスをオンにします。両側のWLANに違いがある場合は、トンネルが切断されます。DMZWLC はトラフィックを拒否します。次のタイミングで確認できます **run debug mobility**.

すべての値は、実際には DMZWLC から取得されます。たとえば、IP アドレスや VLAN 値などです。WLC1 側を個別に設定し、要求を WLCDMZ にリレーします。

ログイン ページ用の証明書

このセクションでは、WebAuthページに独自の証明書を配置するプロセス、または192.0.2.1 WebAuth URLを非表示にして名前付きURLを表示するプロセスについて説明します。

コントローラの Web 認証用の証明書のアップロード

GUI(**WebAuth > Certificate**)またはCLI(転送タイプ **webauthcert**)証明書をコントローラにアップロードできます。

認証局(CA)で作成された証明書であっても、サードパーティの公式証明書であっても、.pem形式である必要があります。

送信前に、証明書のキーを入力する必要もあります。

アップロード後、証明書を有効にするには、リブートする必要があります。再起動したら、GUIのWebAuth証明書ページに移動し、アップロードした証明書の詳細（有効性など）を確認します。

重要なフィールドは、証明書に発行される名前である、Common Name（CN）です。このフィールドについては、このドキュメントの「コントローラ上の認証局などの証明書」セクションで説明します。

リブートして証明書の詳細を確認すると、WebAuthログインページに新しいコントローラ証明書が表示されます。ただし、次の 2 つの状況が発生します。

1. 証明書の発行元が、確実に信頼できる主要ルート CA のいずれかである場合は問題ありません。たとえば、VeriSign です。ただし、通常、Verisign サブ CA や非ルート CA により署名されます。記載されている CA が信頼できるかどうかは、ブラウザで証明書ストアをチェックできます。

2. 小規模な企業/CA から取得した証明書は、すべてのコンピュータで信頼されません。クライアントにも会社/CA証明書を提供し、ルートCAの1つがその証明書を発行します。最終的には、「Certificate has been issued by CA x > CA x certificate has been issued by CA y > CA y certificate has been issued by this trusted root CA」のようなチェーンが作成されます。 最終的には、クライアントが信頼する CA に到達します。

コントローラ上の認証局などの証明書

「this certificate is not trusted」という警告を削除するには、コントローラ上でコントローラ証明書を発行したCAの証明書を入力します。

次に、コントローラは両方の証明書（コントローラ証明書とそのCA証明書）を提示します。CA証明書は、信頼できるCAであるか、CAを検証するためのリソースを持っている必要があります。信頼できる CA に送信される CA 証明書のチェーンを構築できます。

チェーン全体を同じファイルに配置します。ファイルには、次の例のような内容が含まれます。

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

証明書を URL に一致させる方法

WebAuth URL は自身を認証するために 192.0.2.1 に設定され、証明書が発行されます（これは、WLC 証明書の CN フィールドです）。

たとえば、WebAuth URLを「myWLC.com」に変更するには、 **virtual interface configuration** (192.0.2.1インターフェイス)にアクセスし、 **virtual DNS hostname**たとえば、myWLC.comなどです。

これにより、URL バーの 192.0.2.1 が置換されます。この名前は解決できる必要があります。スニファ トレースは、どのように機能するかを示しますが、WLC がログイン ページを送信すると、WLC は myWLC.com アドレスを示し、クライアントはその DNS で名前を解決します。

この名前は192.0.2.1として解決される必要があります。つまり、WLCの管理にも名前を使用する場合は、WebAuthに別の名前を使用します。

WLC管理IPアドレスにマッピングされたmyWLC.comを使用する場合は、myWLCwebauth.comなどの別のWebAuth名を使用する必要があります。

証明書の問題のトラブルシューティング

このセクションでは、証明書問題をトラブルシューティングの確認方法および確認内容について説明します。

確認方法

OpenSSL（Windowsの場合はOpenSSL Win32を検索）をダウンロードしてインストールします。何も設定せずに、binディレクトリに移動して試すことができます **openssl s_client –connect (your web auth URL):443**、

このURLがWebAuthページがDNSにリンクされているURLである場合は、このドキュメントの次のセクションにある「チェック対象」を参照してください。

証明書でプライベートCAを使用する場合は、ルートCA証明書をローカルマシンのディレクトリに配置し、openssslオプションを使用します **-CApath**.中間CAがある場合は、同じディレクトリに配置します。

証明書に関する一般的な情報を取得してチェックするには、次のコマンドを使用します。

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

openssslを使用して証明書を変換することも役立ちます。

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

確認内容

接続時にクライアントに送信される証明書を確認できます。デバイス証明書を読み取ります。CNは、Webページに到達できるURLである必要があります。

デバイス証明書の「issued by」行を参照します。これは、セカンド証明書の CN と一致する必要があります。この2番目の証明書「issued by」は、次の証明書のCNと一致している必要があります（以下同様）。一致しない場合、チェーンは確立されません。

次に示すOpenSSLの出力で、次の点に注意してください。 **openssl** デバイス証明書を確認できません。その「issued by」が、指定されたCA証明書の名前と一致しません。

SSL の出力

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

別の問題として、証明書をコントローラにアップロードできないことが考えられます。この場合、有効期間、CA などは問題ではありません。

これを確認するには、Trivial File Transfer Protocol（TFTP；トリビアルファイル転送プロトコル）の接続を確認し、コンフィギュレーションファイルの転送を試みます。を入力すると、 **debug transfer all enable** コマンドを使用して、証明書のインストールに問題があることに注意してください。

この原因は、証明書で使用されるキーが正しくないことが考えられます。また、証明書のフォーマットが正しくない、または壊れていることも考えられます。

証明書の内容を確実に有効な証明書と比較することをお勧めします。これにより、 **LocalkeyID** 属性は、すべての0を表示します（すでに発生しています）。 その場合、証明書を再変換する必要があります。

OpenSSL では、.pem から .p12 に変換し、目的のキーで .pem を再発行できる 2 つのコマンドが

あります。

証明書とキーを含む .pem を受け取った場合、キーの部分をコピー/ペーストします。 **----BEGIN KEY ---- until ------- END KEY ------** .pemから「key.pem」に移動します。

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ?キーが表示されます。enter **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** その結果、パスワードを含む動作可能な.pemが作成されます **check123**.

トラブルシューティングを行うその他の状況

このドキュメントでは**モビリティ アンカー**については説明していませんが、**アンカー ゲスト**の場合、モビリティ エクスチェンジが正しく発生し、クライアントがアンカーに到達することを確認します。

WebAuth 問題が発生した場合、アンカーでトラブルシューティングを行う必要があります。

次に、トラブルシューティングできる一般的な問題をいくつか示します。

- **ユーザをゲスト WLAN に関連付けることができない**。

  これは、WebAuth に関連するものです。クライアント設定、WLAN のセキュリティ設定、これが有効にされているかどうか、無線がアクティブで機能しているかどうかなどを確認します。

- **ユーザが IP アドレスを取得できない**。

  ゲスト アンカーの場合、これは多くの場合、外部およびアンカーが同じ方法で設定されていない場合に発生します。それ以外の場合、DHCP 設定や接続などを確認します。
- 他の WLAN が同じ DHCP サーバを正常に使用できるかどうかを確認します。これは、WebAuth とは関係ありません。

- **ユーザがログイン ページにリダイレクトされない**。

  これは、一般的な症状ですが、より正確に説明します。この問題が発生する状況は次の 2 つあります。

  ユーザがリダイレクトされない（ユーザが URL を入力しても、WebAuth ページにアクセスできない）。 この場合、次のことを確認します。

  DHCP (**ipconfig /all**!--- インターネット（VPN 以外）上の

  DNSがクライアントから到達可能であること(**nslookup (website URL**!--- インターネット（VPN 以外）上の

  リダイレクトされる有効な URL をユーザが入力している。

ユーザがポート 80 の HTTP URL にアクセスしている（たとえば、http://localhost:2002 で ACS にアクセスするには、ポート 80 ではなくポート 2002 に送信されるまでリダイレクトされません）。

ユーザは、192.0.2.1 に正しくリダイレクトされるが、ページ自体が表示されない。

これは、通常、WLC 問題（バグ）またはクライアント側の問題です。クライアントに何らかのファイアウォール、ソフトウェア、またはポリシーブロックがある可能性があります。また、Web ブラウザでプロキシを設定している可能性もあります。

推奨事項：スニファ トレースをクライアント PC で使用します。ワイヤレス アダプタで実行し、WLC が応答しリダイレクトするか示す Wireshark 以外、特殊なワイヤレス ソフトウェアは必要ありません。この問題には 2 つの原因が考えられます。WLC から応答がないか、WebAuth ページの SSL ハンドシェイクに問題があるかのいずれかです。SSL ハンドシェイク問題については、ユーザ ブラウザで SSLv3 が許可されているかどうか（一部では SSLv2 のみ許可）、また証明書検証での頻度を確認できます。

共通して、DNS なしで Web ページが表示されるかどうかを確認するには、http://192.0.2.1 を手動で入力します。実際、http://10.0.0.0 を入力しても効果は同じです。WLC は、入力された IP アドレスをリダイレクトします。そのため、http://192.0.2.1 と入力しても、Web リダイレクションは回避されません。https://192.0.2.1(secure)と入力すると、WLCがHTTPSトラフィックをリダイレクトしないため、これは機能しません（デフォルトでは、これはバージョン8.0以降で実際に可能です）。 リダイレクトせずにページを直接ロードする最良の方法は、https://192.0.2.1/login.html を入力することです。

- **ユーザが認証できない**。

  このドキュメントで認証について説明しているセクションを参照してください。RADIUS でローカルにクレデンシャルを確認します。

- **ユーザが WebAuth を介して正常に認証できるが、その後インターネットにアクセスできない**。

  WLANのセキュリティからWebAuthを削除し、WLANを開くことができます。次に、Web や DNS などにアクセスできます。ここでも問題が発生する場合、WebAuth 設定も削除して、インターフェイス設定を確認します。

詳細については、以下を参照してください。「ワイヤレス LAN コントローラ（WLC）上の Web 認証のトラブルシューティング」

HTTP プロキシ サーバとその動作方法

HTTP プロキシ サーバを使用できます。192.0.2.1 がプロキシ サーバを通過しない例外をクライアントのブラウザに追加する必要がある場合、プロキシ サーバのポート（通常は 8080）で HTTP トラフィックに対する WLC リッスンを作成できます。

この状況を理解するには、HTTP プロキシの動作を認識する必要があります。これは、ブラウザ

でのクライアント側の設定内容（IP アドレスおよびポート）です。

ユーザが Web サイトにアクセスする場合、通常、DNS で名前が IP に解決され、Web ページから Web サーバに要求されます。プロセスは常にページのHTTP要求をプロキシに送信します。

プロキシは、必要に応じて DNS を処理し、Web サーバに転送します（ページがプロキシでキャッシュされていない場合）。 記述は、クライアントとプロキシ間のみです。プロキシが実際の Web ページを取得するかどうかは、クライアントとは関係ありません。

次に、Web 認証プロセスを示します。

- ユーザが URL を入力します。
- クライアント PC がプロキシ サーバに送信します。
- WLCはプロキシサーバIPを代行受信および模倣します。PCに対して192.0.2.1へのリダイレクトで応答します

この段階で、PC が設定されていない場合、プロキシに 192.0.2.1 WebAuth ページが要求されるので、機能しません。PC は、192.0.2.1 例外を作成する必要があります。次に、HTTP 要求を 192.0.2.1 に送信し、WebAuth に進みます。

認証されると、すべての通信が再びプロキシを通過します。例外設定は、通常、プロキシ サーバの設定同様、ブラウザにあります。次のメッセージが表示されます。「Do not use proxy for these IP addresses」

WLCリリース7.0以降では、この機能は **webauth proxy redirect** グローバルWLC設定オプションで有効にできます。

有効にされると、WLC は、クライアントがプロキシを手動で使用するように設定されているか確認します。この場合、クライアントは、正常に機能するようにプロキシ設定を変更する方法を示すページにリダイレクトされます。

WebAuth プロキシ リダイレクトは、さまざまなポートで機能するように設定でき、中央 Web 認証に対応します。

WebAuth プロキシ リダイレクションの例については、「Web Authentication Proxy on a Wireless LAN Controller Configuration Example」を参照してください。

HTTPS ではなく HTTP での Web 認証

HTTPS ではなく HTTP で Web 認証にログインできます。HTTP でログインする場合、証明書アラートは受け取りません。

WLC リリース 7.2 よりも前のコードでは、WLC の HTTPS 管理を無効にし、HTTP 管理をそのままにしておく必要があります。ただし、この場合、HTTP を介した WLC の Web 管理だけが許可されます。

WLCリリース7.2コードの場合は、 **config network web-auth secureweb disable** コマンドを発行します。この場合、管理ではなく、Web 認証の HTTPS だけが無効になります。この場合、コントローラをリブートする必要があります。

WLC リリース 7.3 以降のコードでは、GUI および CLI を介してのみ WebAuth の HTTPS を有効/無効にできます。

関連情報

- ワイヤレス LAN コントローラの Web 認証の設定例
- ワイヤレス コントローラ WebAuth バンドルのソフトウェアのダウンロード
- カスタマイズされた Web 認証ログイン ページの作成
- ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例
- ワイヤレス LAN コントローラ 5760/3850 の Web パススルーの設定例
- Webリダイレクトの設定(GUI)
- Webリダイレクトの設定(CLI)
- 『ワイヤレス LAN コントローラ (WLC) 上の Web 認証のトラブルシューティング』
- ワイヤレス LAN コントローラ上の Web 認証プロキシの設定例
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。